KERALA LAW ACADEMY LAW COLLEGE

31st All India Moot Court Competition 2022

(9th February to 12th February 2022)

Moot Court Proposition*

Sahu Pal v State of Dharmasthan

1. Dharmasthan is a State in the Indian Union. Nalkir Yashi is the Chief Minister of the State. Centre for Digital Technology (hereinafter "CDT") is an institution registered under The Indian Societies Registration Act of 1860.

2. The Vision of CDT is stated as follows:

> "CDT is envisioned as an organization to bring in innovative technology and its application into public domain. The key mission of the organization is to improve science and development communication through the deployment of needful technological as well as creative aids. Inclusiveness is another major mission of CDT which has been successfully attained through commitment and hard work of years."

3. The Mission of CDT is stated as follows:

> "To become the leading service provider and product innovator in new information technology systems, tools, applications and content development with thrust on deployment of sustainable technology for science and development communication."

---

* The moot proposition is created by Prof. Dr. K.C. Sunny, Vice-Chancellor, National University of Advanced Legal Studies (NUALS), Kochi.

4. The Governing body of CDT has been constituted by the Government with the following members as per section XXV of Article 5 of Memorandum of Association and Rules and Regulations of CDT.

1. Hon'ble Chief Minister of Dharmasthan.
2. Principal Secretary, Finance Department, Government of Dharmasthan.
3. Secretary, Science & Technology Department, Government of Dharmasthan.
4. Director, CDT
5. Registrar, CDT
6. Director, Information & Public Relations Department, Government of Dharmasthan.
7. Vice Chancellor, Technological University, Dharmasthan.
8. Five Persons having Profound knowledge and Practical experience in Information Technology nominated by the Government.
9. One member of the Dharmasthan legislative assembly nominated by the State Government.

5. On 20-07-2021, the leading newspaper, “Dharmasthan Times”, published from the capital city of the State published the following news item.

> "The Government Institution CDT has developed a spyware named as ‘Nososis’. This spyware is a surveillance software, developed in a secret collaboration with an IT firm ‘Shamgular’ registered in Saint Kitts Island. ‘Shamgular’ is a firm known to build sophisticated software and technology for selling solely to law enforcement and intelligence agencies of governments and private firms for the sole purpose of saving lives through preventing crimes and terror acts. ‘Nososis’ software is created in such a manner as to gain access to cell phone without consent and gather personal and sensitive information and deliver it to the user. So, in effect it is spying on third party.

According to IT experts, through this spyware, contacts and browser history can be collected. In addition, a hacker can hijack the phone's microphone and camera, turning it into a real-time surveillance device. According to reliable sources, ‘Nososis’ is a rather complex and expensive malware, designed to spy on individuals of particular interest and so the average user is unlikely to encounter it.

It is a modified version of ‘Pegasus’ spyware which was first discovered in an iOS version in 2016 and then a slightly different version was found on Android. IT experts note that in the early days, one of the main infection schemes was via an SMS. The victim got an SMS with a link. If the person clicks on it, then their device gets infected with the spyware.

Software engineers state that eventually, as the public became more aware of these tactics and were better able to spot malicious spam, zero-click exploit solution was discovered. This method does not rely on the target doing anything at all in order for ‘Nososis’ to compromise their device. Zero-click exploits rely on bugs in popular apps like iMessage, WhatsApp and FaceTime, which all receive and sort data, sometimes from unknown sources. Once a vulnerability is found, ‘Nososis’ can infiltrate a device using the protocol of the app. The user does not have to click on a link, read a message, or answer a call — they may not even see a missed call or message. “It hooks into most messaging systems including Gmail, Facebook, WhatsApp, FaceTime, Viber, WeChat, Telegram, Apple's inbuilt messaging and email apps and others. With a line-up like this, one could spy on almost the entire world population. It's apparent that NSO is offering an intelligence- agency-as-a service,” a former Director of an IT company said.

Apart from zero-click exploits, there is another method called “network injections” to quietly access a target's device. A target's Web browsing can leave them open to attack without the need for them to click on a specifically-designed malicious link. This approach involves waiting for the target to visit a website that is not fully secured during their normal online activity. Once they click on a link to an unprotected site, the NSO Group's software can access the phone and trigger an infection."

6. On 28-07-2021, another newspaper, “Dharmasthan Voice”, published a story containing the following details regarding ‘Shamgular’.

> "Shamgular claims that they develop the best-in-class technology to help government agencies detect and prevent terrorism and crimes. In addition, their products help licensed government intelligence and law-enforcement agencies to lawfully address the most dangerous issues in today’s world. Technology has helped prevent terrorism, break up criminal operations, find missing persons and assist search and rescue teams. Shamgular’s products are used exclusively by government intelligence and law enforcement agencies to fight crime and terror. The products are used to
>
> - Prevent terrorism, including gun violence, car bombs, and suicide bombers at transportation hubs, public parks, markets, concert venues, sports arenas, and other public areas.
> - Break up pedophilia, sex- and drug-trafficking rings, and money-laundering operations.
> - Find and rescue kidnapped children.
> - Assist emergency search and rescue (SAR) teams in locating survivors trapped under collapsed buildings in the wake of natural disasters or construction failures".

7. On 29-07-2021, another newspaper, “Dhamasthan Reporter”, published the news item that the phone numbers of over 42 journalists were on a hacking list of an unidentified agency using the spyware ‘Nososis’. The report said that forensic tests have confirmed the presence of the military-grade spyware on some devices. Those on the list of potential targets included journalists of national and local dailies and news channels. The analysis of the data showed that most of the journalists were targeted between 2018 and 2019.

8. On 30-07-2021, “Dhamasthan Voice” published the following news regarding the operation of ‘Nososis’.

> "As soon as the spyware is installed on a mobile device, it starts getting in touch with the “command and control servers” of the operator. It can then follow instructions and send private data available on the mobile device which includes text messages, event schedules, contacts, passwords, voice calls on messaging apps, location data etc. The spyware also has the potential to turn on the phone camera and microphone, and spy on an individual’s calls and activities.
>
> One of the prominent features of ‘Nososis’ is the “Zero Click attacks”. The Zero-Click infection means that the individual is not even required to open a link for them to be attacked with the malware. It gets installed by missed call or a message. After the installation on a mobile device is complete, ‘Nososis’ can use some bypassing techniques in order to read encrypted messages on encrypted messaging apps such as Signal, WhatsApp, Telegram etc."

9. On 02-08-2021, CDT published a press release stating that the newspaper reports regarding ‘Nososis’ are false and misleading. It was stated that "The report by Forbidden Stories is full of wrong assumptions and uncorroborated theories that raise serious doubts about the reliability and interests of the sources. It seems like the unidentified sources have supplied information’s that have no factual basis and are far from reality"

10. On 03-08-2021, the leader of the opposition in the Legislative Assembly alleged that CDT had sold ‘Nososis’ to Dhamasthan police and the Police Department is using it for detection of crimes and for collecting information regarding the political opponents, religious leaders and journalists . However, the Chief Minister denied the allegations. On 04-08-2021, at 12 pm, the Leader of the Opposition visited the Governor of the State and asked for CBI Enquiry on ‘Nososis’ scandal. In the meantime, on 04-08-2021, at 4 pm, the meeting of the

State Cabinet decided to withdraw the general consent given to the CBI for enquiry in the State, through the notifications of the Government of Dharmasthan under Section 6 of the Delhi Special Police Establishment Act 1946.

11. On 10-08-2021, Mr. Sahu Pal, the editor of "Dharmasthan Times", filed a petition before the High Court of Dharmasthan under Art 226 of the Constitution. It was alleged that the Government is infringing the privacy of citizen by the unlawful use of 'Nososis'. It was contented that his own privacy was violated. The newspaper reports regarding the use of 'Nososis' and a forensic analysis report, stating that Mr. Sahu Pal's phone showed clear signs of 'Nososis' spyware activity between February 2020 and January 2021, were attached in the petition.

12. The writ petition filed by Mr. Sahu Pal's contained the following prayers.

1. The Court may direct the CBI investigation to prosecute all persons, who committed offences by way of using 'Nososis'.

2. Government may be directed to produce all documents related to 'Nososis' before the High Court.

3. An amount of Rs 50 lacks may be awarded as compensation for violation of his privacy.

13. Subsequently, some other aggrieved persons also filed writ petitions before the Dharmasthan High Court identical to the one filed by Mr. Sahu Pal.

14. On 06-09-2021, the government filed an affidavit which neither confirmed nor denied the use of the spyware to hack phones of others and offered to set up an expert committee to enquire into all issues. The full bench headed by the Chief

Justice asked to file a detailed affidavit stating whether there was infringement of privacy of anybody or not. On the next day, the Advocate General (AG) of the State appeared before the full bench and emphasized that the government is open to have a committee of independent domain experts who can go into all aspects of the controversy and submit its report before the Court. But the use of a particular software “cannot be made a part of the public discourse in the larger interest of the State and in the interest of the security of the State". But the bench was not impressed with AG's contentions. The Chief Justice pointed out that "We said it very clearly even on the last date that nobody is interested in disclosure of information that could compromise the security of the State. We wanted a limited affidavit from you because we have petitioners before us, citing violation of their privacy. In the face of the allegations that some software was used to snoop on certain individuals like the petitioner, it has to be made known whether there are methods of interception other than lawful means". Chief Justice added: “In your affidavit, you could clarify whether there was a lawful interception of the petitioners or not. And if there was any unlawful interception that was not in your knowledge, then it should be a matter of your concern, too". However, the AG was quick to clarify that the court’s opinion about him in the matter was not correct. According to him, the information sought by the petitioners was “sensitive” in nature and concerned “security of the state”.

15. On 10-09-2021, the AG filed an affidavit claiming that the protection under Sections 123 and 124 of Indian Evidence Act may be granted to the government documents related to ‘Nososis’. On 20-09-2021, Mr. Sahu Pal filed another petition challenging the constitutional validity of Sections 123 and 124 of the Indian Evidence Act. Full bench decided to hear both the petitions together.

16. Thereafter, several other writ petitions came to be filed in other States in the Indian Union on identical set of facts challenging alleged State intrusion on privacy using identical software. Since then, identical writ petitions also came to be filed directly before the Supreme Court of India under Article 32 of the Constitution of India. The Bench of the Chief Justice of the Supreme Court noticing the pendency of identical matters before various High Courts and holding that the matters including issues of right to privacy under Article 21 of the Constitution of India vis-a-vis national security and constitutional validity of Sections 123 and 124 of the Indian Evidence Act, constitute matters of great public importance for the entire nation, ordered transfer of all writ petitions in these matters pending in various High Courts to the Supreme Court to be heard along with the identical writ petitions filed before the Supreme Court. It was decided to hear the two writ petitions filed by Mr. Sahu Pal of Dharmasthan State, as the lead case. The lead case and connected cases are posted to 12.02.2021 for final hearing before the Supreme Court of India.

[Note : The participants are required to argue only for and against the writ petitions filed by Mr. Sahu Pal, being the lead case. Only one combined written memorial consisting of issues contained in both writ petitions of Mr. Sahu Pal need to be submitted i.e., each team to prepare one combined memorial for the petitioner, Mr. Sahu Pal and one combined memorial for the respondent, State of Dharmasthan.]